Core 2000 Interface Version 2.30

User Manual

Revision 1

Core Integrated Systems

Time & Data Systems

Contents

Introduction **3**

Audience 3
Features 3

Installation **6**

Requirements 6
Installation 9

Configuration **11**

Scope of User Configuration 11
Navigation 11
Configuring the Oracle Logon 11
Configuring the Software to run as a Service 13
Synchronising the Date and Time 15
Importing T&A Bookings During a Parallel Run 16
Enforcing Expiry Dates 17
Reformatting T&A Balances 18
Configuring Message Notification 19
Configuring an Automatic Roll Call Report 20
Setting the User Password 22
Amending Hardware Device Details 23

Maintenance **27**

The Main Program Window 27
Starting and Stopping the Software 31
Checking the Status of the Oracle Connection 32
Checking the Status of the ADACS 5 Connection 34
Checking the Hardware Communication Status 35

Database Synchronisation **37**

Technical Background 37
The Download Terminal Data option in Core 38
The Database Download Option 40
The Full Reconciliation Option 41

Backup and Recovery **42**

Files and Directory Structure 42
Backing Up 43
Restoring a Backup 44
Re-importing Bookings into Oracle 47

Additional Information **49**

Online vs. Offline Mode 49
Hardware Compatibility Implementation 50

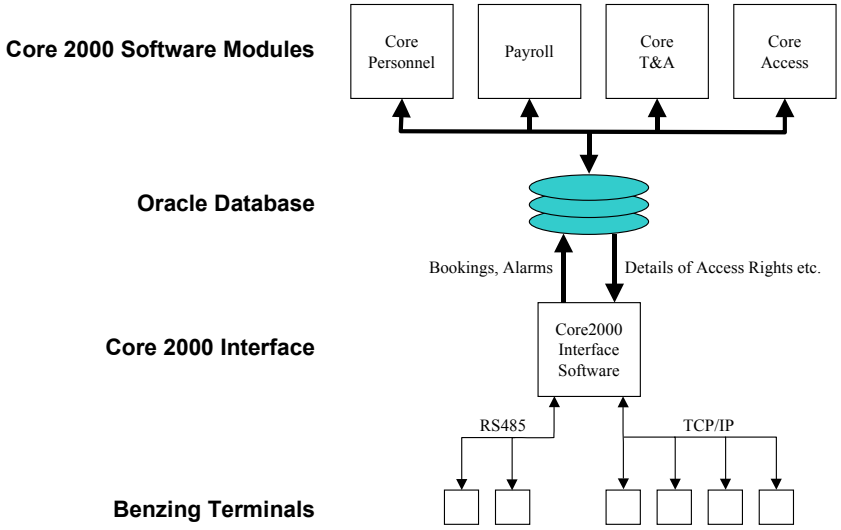
Introduction

Audience

This manual is intended for customers. Since it describes a back-end server process it will be of interest to staff in the IT department, rather than security guards or the HR department.

Features

The Core 2000 Interface implements the communication between the Core 2000 software suite and the access control and T&A card readers. It typically runs continuously as a service process on the database or application server. The following diagram illustrates where the software fits in with regard to the other components of the system:



The software uses a native Oracle SQL Net client to connect to Oracle and can be deployed on the database server, application server or a separate machine. It can connect with a variety of Benzing terminals via RS232/RS485 serial and/or TCP/IP-based network connections. It also supports an optional TCP/IP link to the ADACS 5 software which in turn allows connecting ZMP devices to the system.

It is worth noting that the hardware devices in the Core architecture feature an amount of local intelligence which allows them to keep working independently, if communication with the software breaks down. For instance the Benzing terminals and ZMP devices can store a list of badges and time zones when personnel are permitted access at a reader. It is the job of the Core 2000 Interface to synchronise the content of the Oracle database with the hardware devices and vice versa. It thus has two main functions:

- To transmit data such as access rights, originating from user changes to the Oracle database, to the hardware devices.

- To store events originating at the hardware devices in the Oracle database. Typical events include bookings, when a person presents a card or key-fob to the device, and alarm conditions, such as when a door is wedged open[1].

The Core 2000 Interface is designed to operate fully automatically, collecting events from the hardware devices and storing them in Oracle within seconds of their origin and, through the use of database triggers, transmitting changes that users made in the Oracle database to the hardware within seconds.

It features fault-tolerant operation. For instance, if the connection to a Benzing terminal breaks down due to a network failure, the Benzing terminal buffers events and automatically transmits them when communication with the Core 2000 Interface is re-established. Similarly the Core 2000 Interface buffers changes in access rights and other changes originating in Oracle and transmits them to the hardware when it is communicating again. A similar principle applies should it lose connection to Oracle, for instance if the Oracle database is taken down. In both cases of communication loss, with the hardware or with Oracle, the Core 2000 Interface automatically re-establishes communication when possible and synchronises the outstanding data.

Besides data synchronisation the software features the ability to validate and authorise bookings in real time. When this happens the Benzing terminals are said to be configured in online mode. When a booking is attempted, the terminal transmits it to the Core 2000 Interface, then waits for a response from the software before authorising the booking. This allows implementation of features not possible through local intelligence, such as global (site-wide) anti-passback.

The software is optimised to guarantee a quick and consistent response to terminals in online mode, typically within one second. It's main measure to achieve this is to cache

[1] The exact nature of possible events depends on the hardware and parameterisation of the hardware by our engineers.

details of badges and access rights in memory and the local hard disk, rather than consulting the Oracle database directly to respond to bookings. Thus there are actually two layers of local intelligence beneath the Oracle database, the Core 2000 Interface and the hardware devices. This also has the benefit that, if the Oracle database is shut down, the Core 2000 Interface can keep running and continue to enforce features such as site-wide anti-passback.

Installation

Requirements

Recommended machine specification

The software can be installed on the database server (recommended) or application server, or it can be installed on a dedicated machine. In the latter case this should still be a server-type machine in the IT department, rather than a machine used for other tasks in a general office space, and the recommended specification for an installation in a company with up to 3,000 employees and 50 Benzing terminals is:

Processor:	Pentium II 300 or better.
Memory:	128Mb.
Disk:	4Gb disk with at least 1Gb free space.
Graphics:	SVGA, 800x600, 256 colours.
Network:	Ethernet or Token Ring, TCP/IP.
Modem:	V90 (56 kbps). Either this modem should be fitted in the machine itself or there should be dial-up networking access to the company network. The modem should be connected to a phone line that can be direct-dialled from outside and that can dial back to outside numbers.
Ports:	At least one available serial port, if Benzing terminals are connected via serial interface, rather than network.
OS:	Windows 2000 or Windows NT 4.0, SP4 or higher.
Remote S/W:	pcANYWHERE 8.0 or later.

In a company with more than 3,000 employees and/or 50 Benzing terminals a faster CPU and high-speed disk (>= 7,200RPM) is recommended. Memory and disk space requirements should be calculated as described below.

Minimum machine specification

The minimum machine specification is:

Processor:	Pentium 150 or better.
Memory:	64Mb.
Disk:	2Gb disk with at least 500Mb free space.
Graphics:	VGA, 640x480, 16 colours.
Modem:	V34 (33.6 kbps).
OS:	Windows 95/98/Me/2000 or NT 4.0, SP4 or higher.
Remote S/W:	pcANYWHERE 8.0 or Laplink 7.0 or later.
Other:	Same as the recommended machine specification.

Please note: A machine such as this would obviously be old. Since the Core 2000 Interface is a mission-critical application you should satisfy yourself that the machine is still reliable. Also note that the software performs significantly better under Windows NT/2000.

Memory requirements

The maximum amount of memory used by the software can be estimated as follows:

$9{,}000{,}000 + e \bullet 400 + e \bullet g \bullet 120$ bytes

where e is the total number of employees, contractors and visitors, and g is the number Benzing groups. A Benzing group, which is not related to access groups in CoreAccess, includes between 1 and 60 Benzing terminals, though typically 10 or less. As an example consider a company with 3,000 employees, 50 terminals and 10 terminals per group. There would thus be 5 Benzing groups and the required memory calculation would be:

$9{,}000{,}000 + 3{,}000 \bullet 400 + 3{,}000 \bullet 5 \bullet 120$ bytes = 12,000,000 bytes = 12M

Please bear in mind that the total amount of memory in the machine must also cater for the overheads of the operating system and other running applications.

Disk space requirements

The software automatically logs all communication traffic for a period covering the preceding month (31 days). The bulk of the logged data consists of the bookings made by personnel at the terminals[2]. The amount of required disk space can be estimated as follows:

$m + b \bullet 31 \bullet 400$ bytes

where m is the amount of memory used by the application, as calculated above, and b is the number of bookings per day. For instance, if you take the above sample company again and assume a daily volume of 12,000 bookings, the estimated disk space requirement is:

12,000,000 + 12,000 • 31 • 400 bytes = 160,800,000 bytes = 160M

Oracle client software requirement

The Core 2000 Interface requires Oracle SQL Net client software to access the Oracle database. If installing on the database or application server, this will already be present. If installing on a dedicated machine this can be fulfilled by installing a standard Core client (not a web or Citrix client). The Core 2000 Interface is able to utilise SQL Net 2.3 (Oracle 7.3), 8.0 (Oracle 8.0) or 8.1 (Oracle 8.1) and can connect to an Oracle 7.3, 8.0 or 8.1 database. It is recommended that it use the same version of SQL Net client as the database version. At the time of writing the database version is typically 8.1.6 or 8.1.7 whereas the Forms and Reports 6i Core client installation deploys SQL Net 8.0.6 on the client machines and application server. In this situation it is recommended to install SQL Net 8.1.6 or 8.1.7 in addition to the Core client and use the Oracle 8.1 version of the Core 2000 Interface.

Core client software requirement

If you will use the Core 2000 Interface to automatically run fire alarm-activated roll reports, a standard Core client must be installed on the machine (not a web or Citrix client), including, in particular, the Oracle reports runtime package.

Single installation per machine requirement

You may install and run a single copy of the software per machine. It does not allow running multiple copies or setting up multiple NT/2000 services. In case you need to deploy several copies, for instance for a live and a test environment, you must currently install the second copy of the software on a separate machine.

[2] The purpose of the log files is twofold. Firstly they provide a backup that can be re-imported into the Oracle database, if required. Secondly they include audit information for software support.

Installation

The software is normally installed and configured by our service engineers when the hardware is installed. For re-installation, please refer to the Backup and Recovery chapter on page 42 first.

Logon

You should log on as a user with local administrator rights when installing the software[3].

Installation location

The software must be installed on a local hard drive, not a network drive. When choosing a drive you should take the Disk space requirements on page 8 into account, bearing in mind that these are estimates. If there are multiple local drives or partitions you should avoid the C: drive, since this partition is often the smallest. You should create a new directory to install the software in. A typical installation location is D:\Corinio, provided D: is a local hard drive.

Program installation

The software consists of a single .EXE file and can in many cases be installed without having to reboot the machine. It comes in 4 different versions:

Corinio1.exe:	Uses an Oracle 8.1 client to connect to Oracle.
Corinio8.exe:	Uses an Oracle 8.0 client to connect to Oracle.
Corinio7.exe:	Uses an Oracle 7.3 client to connect to Oracle.
Corinio.exe:	Does not connect to Oracle. This version can be used to begin configuring the software and test hardware communication when Oracle is not yet installed. It must later be replaced with one of the other versions.

To install the software choose one of the above .EXE files and copy it into the installation directory on the hard disk. Please refer to the Oracle client software requirement section on page 8 to choose the correct file. At the time of writing the most commonly installed version is Corinio1.exe.

Note that the software will create additional files and subdirectories in the installation directory, but not elsewhere.

Tip ☞

If the program does not run, but displays a message such as 'Unable to find a required component SQLLIB18.DLL, SQLLIB80.DLL or ORASQL8.DLL', the version of Corinio*n*.exe you're trying to run does not match your SQL Net client version or the SQL Net client is not installed yet. Make sure that you installed the SQL Net client first and rebooted the machine, if asked to do so by the Oracle installation

[3] This is required in order to install the software as a service.

program. In case the client software is installed you may be trying to run the wrong version of the Core 2000 Interface. Try running Corinio8.exe or Corinio7.exe instead of Corinio1.exe or vice versa.

Common controls update

When you first run the Core 2000 Interface, it may ask you to install the latest Microsoft common controls. In this case run the supplied 50comupd.exe program. You will be asked to reboot the machine.

Depending on the existing common controls version, the Core 2000 Interface may run without performing this update and can be used until such time when it's convenient to reboot the machine. However it will be missing the filter-bar user interface feature and, because of the reminder message at program start, it will not start properly as an NT/2000 service.

Technical Background: The Core 2000 Interface requires version 5.80 or later of comctl32.dll. This version is already present in Windows 2000 or if you installed Internet Explorer 5 or later. Otherwise the Microsoft-supplied 50comupd.exe program allows updating this single DLL, without upgrading to Internet Explorer 5.

Icon creation

For easy access to the Core 2000 Interface right-click on the desktop, select New➔Shortcut and create a new shortcut labeled 'Core 2000 Interface' pointing to the program, for example to D:\Corinio\Corinio1.exe.

Configuration

Scope of User Configuration

The software is normally configured by our service engineers at installation time and contains many options that require detailed knowledge of the hardware or that require hardware configuration steps to be performed that match the settings chosen in the software. Such options are beyond the scope of this manual. This chapter only covers options that you can amend safely.

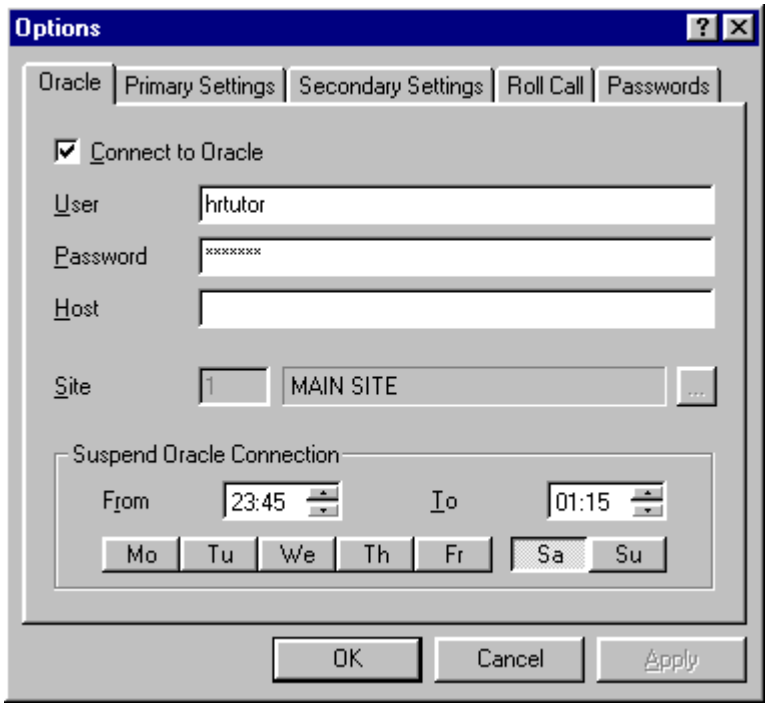
Navigation

Many of the following options are configured via the **Options**... dialog on the **Tools** menu. This dialog can only be invoked when the software is stopped, i.e. not actively communicating with the hardware devices or Oracle, otherwise it is greyed out. For more information, please refer to Starting and Stopping the Software on page 31.

Configuring the Oracle Logon

Objective To specify the Oracle database and user that the Core 2000 Interface should access.

Navigation Select **Options**... from the **Tools** menu and go to the **Oracle** tab.



Connect to Oracle Turn this option on to enable connection to Oracle. If this is turned off, the software does not connect to Oracle when you start communication, though it still attempts to do so in other cases, for instance to save configuration options from this dialog. This option should normally be switched on.

User Specifies the Oracle user.

Password Specifies the Oracle password.

Host Specifies the Oracle host string, sometimes also called the database alias. If the Core 2000 Interface is installed on the database server, this can usually be left blank. For more information, please refer to your Oracle documentation.

Suspend Oracle Connection This option should be used, if the Oracle database is regularly shut down, for instance when it is backed up. It instructs the Core 2000 Interface to log off Oracle at those times in an orderly fashion. As an example, the above screenshot shows it configured to log off from 23:45 on Saturdays until 01:15 on Sundays. If you do *not* want to use this feature, simply make sure none of the weekday buttons are depressed.

Notes Should an Oracle logon fail or if the Connect to Oracle option was deselected, the software automatically synchronises all outstanding data, once the Oracle connection is re-enabled and established again.

In an existing installation you must not change the user and/or host so that the Core 2000 Interface connects to a different database or different set of database tables, for instance by switching from a live user to a test user. If both a live and test environment are required simultaneously, it is recommended that two copies of the software be deployed instead.

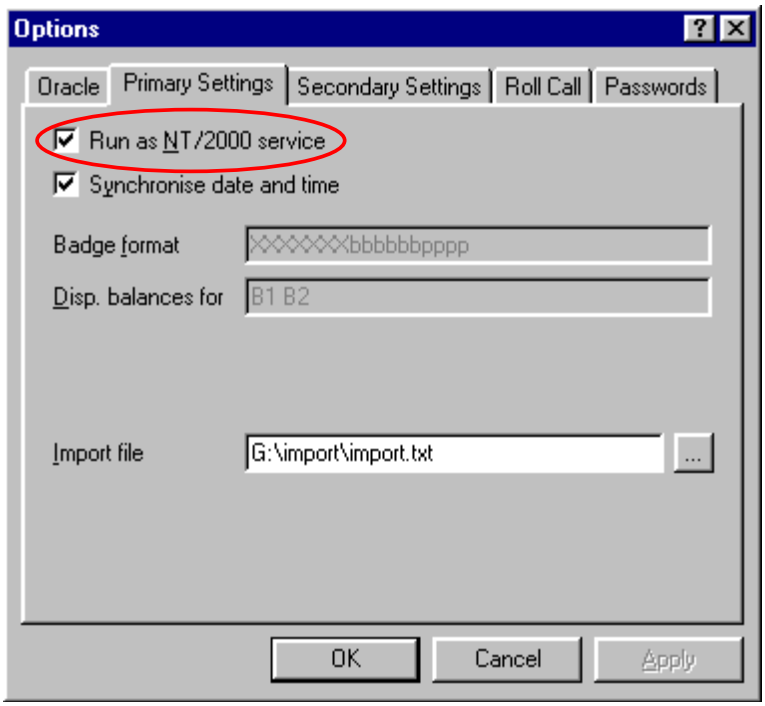
Configuring the Software to run as a Service

Objective To run the software as a service.

Rationale This allows the software to run automatically when the machine boots and to keep running when no user is logged on to the machine.

Platform This option is only available under Windows NT and 2000.

Navigation Select **Options**... from the **Tools** menu and go to the **Primary Settings** tab.



Run as NT/2000 service

To install the software as a service, simply turn this option on as shown in the screenshot, then press **Apply**. This installs it as an automatic service, running in the local system account with the 'Interact with desktop' feature turned on. You can verify the service is installed by examining the Services option in the Windows Control Panel (Control Panel / Admin Tools under Windows 2000). Look for the Core 2000 Interface service.

It is recommended to leave the service configured as an interactive one. In that case, when you run it, a small Core 2000 Interface icon ( ) appears in the status area (sometimes called the system tray) of the taskbar. Click on the icon to start the user interface of the software. You may be asked for a password.

Once the program is installed as a service and you press the Start button, the program disappears and then starts itself as a service. Please refer to Starting and Stopping the Software on page 31 for more information.

You may use the 'net start' and 'net stop' commands to start and stop the service, but it is recommended to leave it running at all times, even if Oracle is shut down. To make sure the program logs off cleanly from Oracle prior to a scheduled Oracle shutdown, you should use the Suspend Oracle Connection option discussed on page 12.

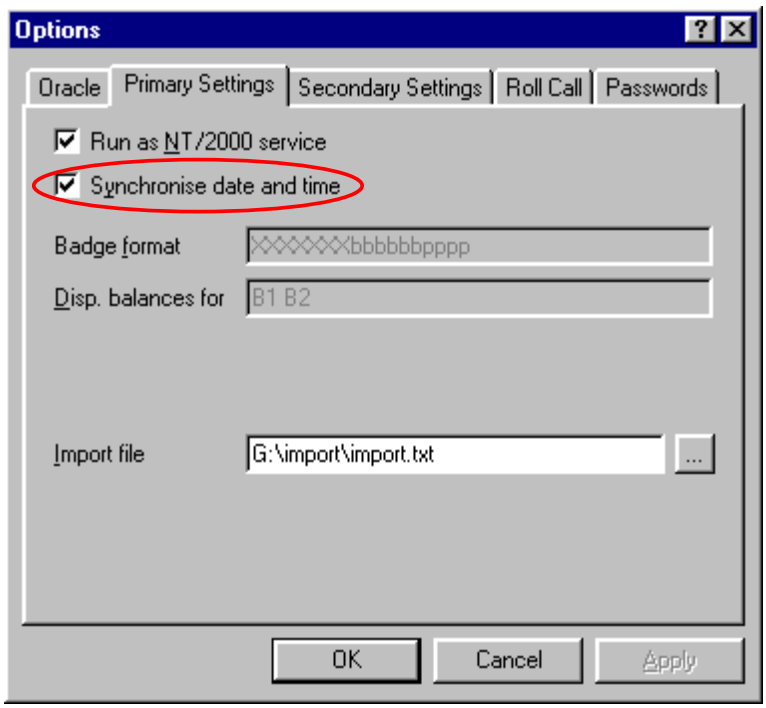
Synchronising the Date and Time

Objective

To automatically synchronise the date and time of the Benzing terminals to the current date and time of the machine running the Core 2000 Interface software.

Navigation

Select **Options**... from the **Tools** menu and go to the **Primary Settings** tab.



Synchronise date and time

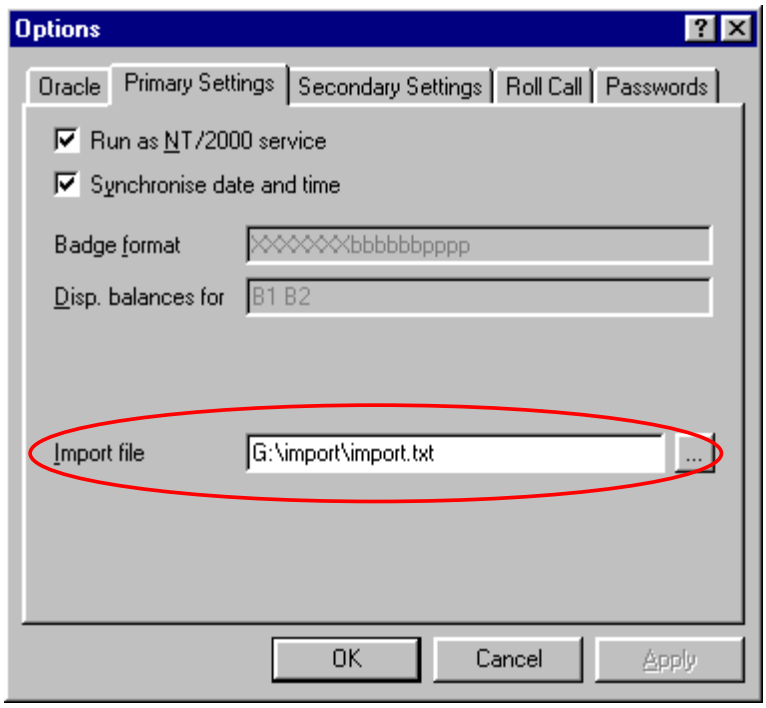
This option causes the Core 2000 Interface to automatically synchronise the clocks in the Benzing terminals to the clock of the machine running the Core 2000 Interface, approximately once every hour. When you turn this option on you must insure that the date and time of the machine is always correct. Instead of using the option you can also run the **Synchronise Date and Time** option on the **Tools** menu for a once-off synchronisation of the date and time.

Note that, if the software is linked to ADACS 5, the clock of the Core 2000 Interface PC/server may itself be synchronised to the ADACS 5 server.

Importing T&A Bookings During a Parallel Run

Objective In case you are upgrading from a legacy system, this option allows you to automatically import Time & Attendance bookings from that system into Core 2000.

Navigation Select **Options**... from the **Tools** menu and go to the **Primary Settings** tab.



Import file Specifies the file containing T&A bookings from the legacy system. This must be a text file in the raw Benzing format. Details are available on request.

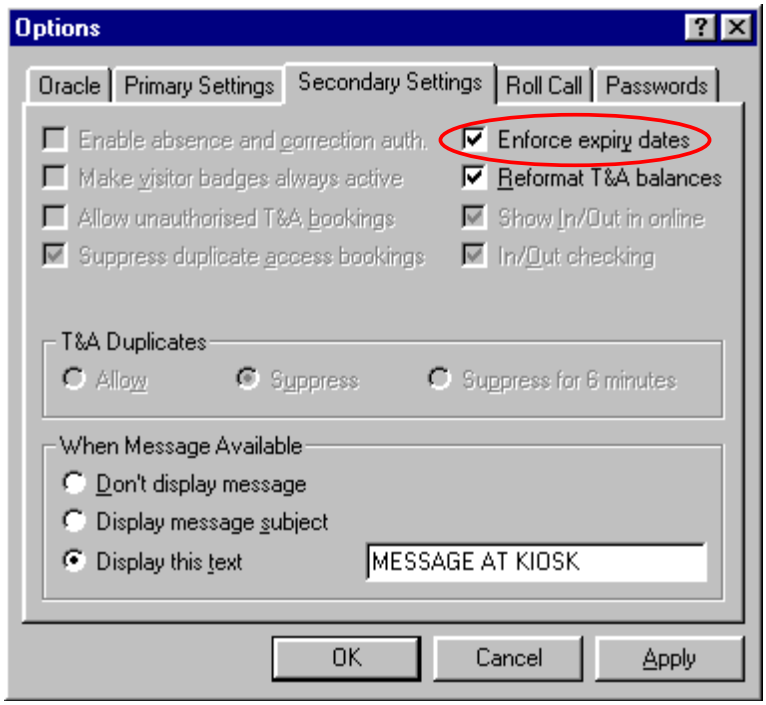
If a filename is given, the software automatically checks for the existence of the file every minute. The file may reside on a local or network drive. If found, it renames the file to <filename>.c2i, to avoid multi-user access conflicts, then imports the .c2i file, then deletes it.

If you do *not* wish to use this option, you should leave the filename blank.

Enforcing Expiry Dates

Objective To enforce the expiry dates entered against badges in CoreAccess.

Navigation Select **Options**... from the **Tools** menu and go to the **Secondary Settings** tab.



Enforce expiry dates Specifies whether to enforce the expiry dates entered against badges in CoreAccess. If this option is selected and an expired badge is used, it is rejected. Badges expire at midnight at the end of the expiry date.

This option globally affects all badges that have an expiry date. You can change it at any time, but like all options in this chapter it is usually set at installation time and not changed thereafter. Depending on the configuration of terminals and total number of expired badges in the system, it may take between one minute and several hours before a change in this option takes full effect.

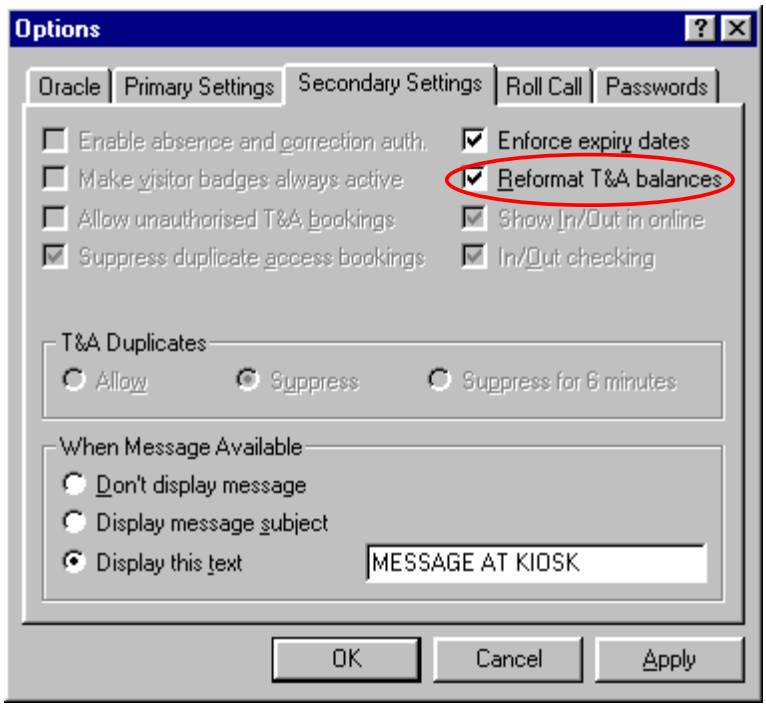
Also note that your Time & Attendance terminals may not be configured to enforce access rights. Such terminals do not enforce expiry dates.

Reformatting T&A Balances

Objective Some installations allow employees to view their flexitime balances at Benzing terminals. The Core 2000 Interface can be configured to change the format that these balances are displayed in.

Scope This option applies when balances are displayed at standard Benzing terminals. It does not apply to the information booth functionality available at Bedanet touch-screen units.

Navigation Select **Options**... from the **Tools** menu and go to the **Secondary Settings** tab.



Reformat T&A balances The standard format that T&A balances are displayed in may show a decimal point between the hours and minutes and may not show a leading zero before the decimal point. If you turn the Reformat T&A balances option on, such balances are reformatted with a colon between the hours and minutes and a leading zero, if applicable. For instance '.20' is changed to '0:20'.

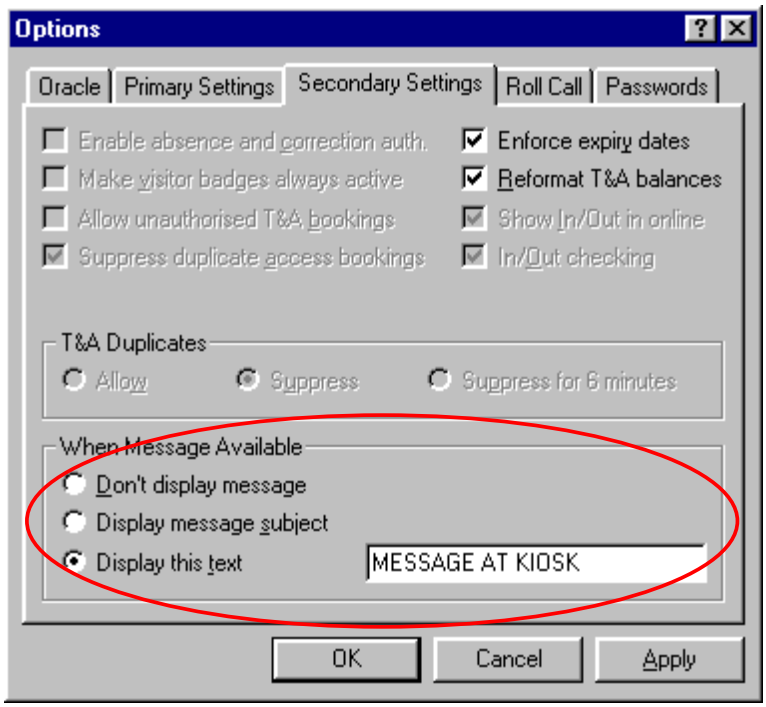
A change in this option comes into effect the next time T&A balances are recalculated and downloaded from Oracle to the Core 2000 Interface. To expedite this process, run the **Access Control / Download Terminal Data / Download All** option in Core[4].

Configuring Message Notification

Objective To display a notification at standard Benzing terminals when a message is available at a Bedanet touch-screen device.

Rationale You can enter messages in Core, for each employee, that can be displayed at Bedanet touch-screen terminals. If a new message is available, employees can be notified, when they use their badge at other terminals, to go to a touch-screen terminal and view the message.

Navigation Select **Options**... from the **Tools** menu and go to the **Secondary Settings** tab.



[4] The Core software may display a warning that it is dangerous to run the Download All option. This is no longer the case with the current version 2.xx Core 2000 Interface software, but only applied with version 1.xx.

Don't display message The employee is not notified when a new message is available.

Display message subject When a new message is available and the employee uses his/her badge at a Benzing terminal, the first 20 characters of the message subject are displayed. If there are several new messages available for an employee, the subject of one of those messages is displayed at random.

Display this text When a new message is available and the employee uses his/her badge at a Benzing terminal, the text entered to the right is displayed. This should direct them to go to a touch-screen terminal and can be a maximum of 20 characters.

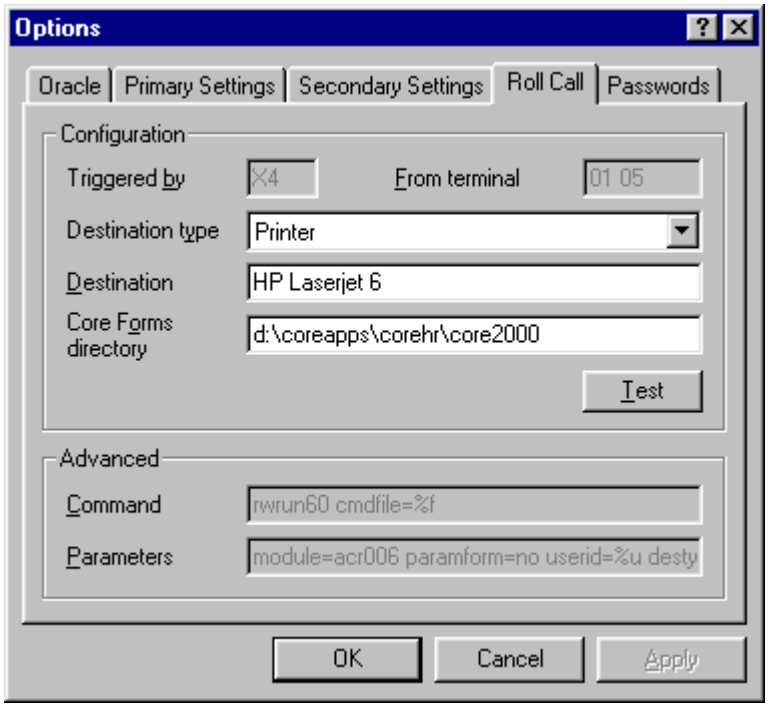
Notes Standard Benzing terminals have a 2-line display of 20 characters each, a 1-line display (older models) or no display at all. The notifications are only displayed on models with a 2-line display, on the second line. Furthermore they are only displayed when the employee makes a valid booking, since otherwise the second line shows an error message.

The notifications keep being displayed until the employee goes to a touch-screen terminal and marks the message(s) as having been read.

Configuring an Automatic Roll Call Report

Objective The Core 2000 Interface can automatically produce a roll call report based upon an event received from a Benzing terminal, such as when a fire alarm is activated. If the automatic roll call feature has been installed by your supplier you can amend the printer settings and produce a test report.

Navigation Select **Options**... from the **Tools** menu and go to **Roll Call** tab.



Destination type Select **Screen**, **Printer** or **File**. Typically the Core 2000 Interface is running on a server in the IT department and a network printer is selected. The **Screen** option is usually not useful, except for testing.

Destination Enter the printer name or filename. Printer names must be entered as they appear in the Windows Printers folder.

Core Forms Directory This must be the directory where the Core 2000 forms are located, e.g. the .fmx and .rep files.

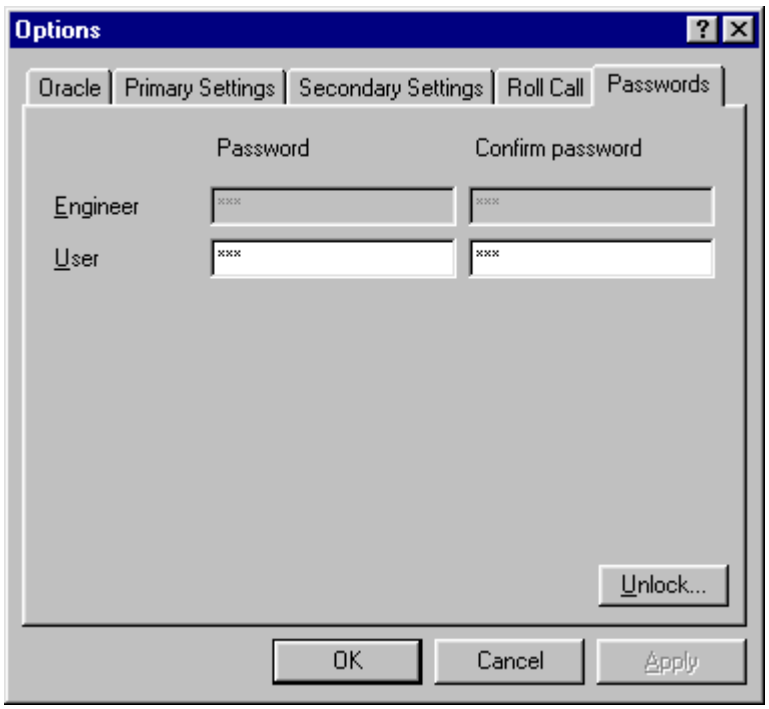
Test This button runs a report to test the current settings.

Notes When a report is triggered, any doors marked as having to be opened or blocked in an emergency are opened or blocked, as specified by the In Emergency option on page 24. However the **Test** button does not invoke this functionality.

Setting the User Password

Objective To restrict access to the software to authorised users only.

Navigation Select **Options**... from the **Tools** menu and go to **Passwords** tab.



User Enter the user password in the **Password** column and repeat the same password in the **Confirm Password** column.

Notes The software features two levels of password security. The engineer password permits full access to service engineers, whereas the user password permits access to only those features that may safely be used by customers themselves. You may leave both passwords blank, set the engineer password alone, or set both passwords.

If the password(s) are set, you are asked to enter a password when you try to run a protected option. For convenience, if you successfully entered a password and hardware and Oracle communication is currently stopped, other options from then on remain unlocked until the software is quit or hardware / Oracle communication is started again. See Starting and Stopping the Software on page 31.

The **Unlock**... button prompts you to type in the engineer password to gain full access to the software.

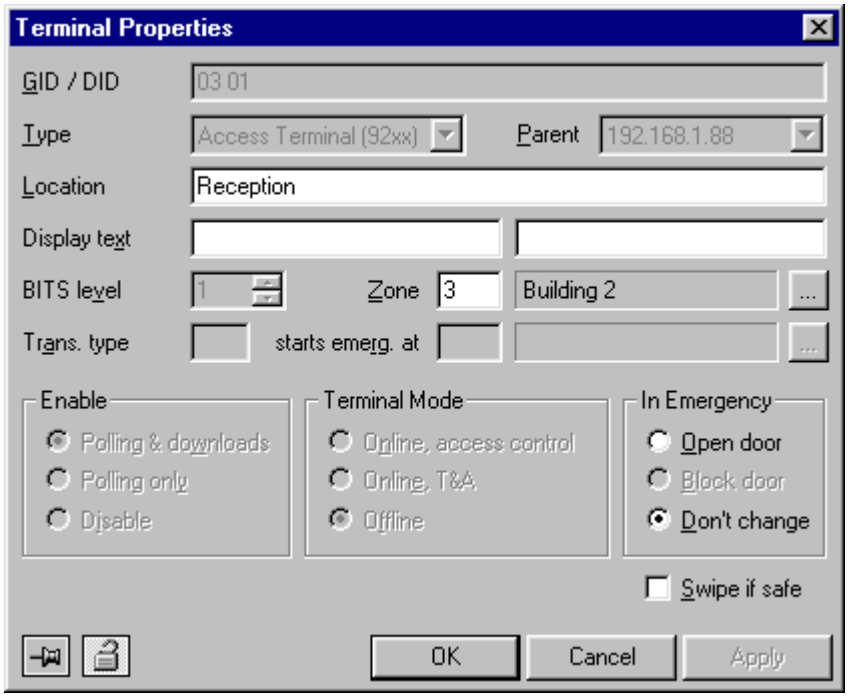
Amending Hardware Device Details

Objective

To configure parameters relating to hardware devices, such as Benzing terminals, Benzing Ethernet adapters and ZMP devices. These are normally configured by our service engineers and you require the engineer password to delete them or set up new ones. As a user you may amend certain details, such as the device descriptions.

Navigation

Go to the **Devices** tab in the main window and double-click on a device. Device details can only be amended when hardware and Oracle communication is stopped, otherwise you are merely able to view them.



Location Specifies the location or description where the device is installed. Typical locations might include Reception, Turnstile 1 IN, Turnstile 1 OUT, Building 502 and so on. The location entered here is shown in CoreAccess, for instance when viewing the access log or when setting up access groups.

Display text Specifies the two lines of text, up to 20 characters each, that are shown on the terminal display when waiting for a badge to be presented. A typical text is 'Present Card' on the first line and the company name on the second line. The texts entered here are only used when the Swipe if safe option is enabled, otherwise they may be left blank, as shown in the screenshot. In that case the texts are configured elsewhere by our service engineers.

Zone Specifies the zone or site that the terminal is installed at. Use the ... button to browse.

In Emergency Specifies whether the door should automatically be opened or blocked in an emergency. If the door is opened, the magnetic lock is released and personnel need not use their badges to go through the door or turnstile[5]. This allows quicker evacuation. If the door is blocked, no one is allowed to go through the door or turnstile, even with a badge. This option might be used to block turnstiles in the in-going direction to prevent additional personnel entering the site in an emergency. The Don't change option causes no change in the operation of the door or turnstile in an emergency.

This option is triggered when an emergency for the zone that the terminal belongs to is started in CoreAccess or when an automatic roll call report is triggered (via the fire alarm).

Swipe if safe Specifies whether this terminal may be used to 'swipe safe' in an emergency. This means the terminal is installed at an assembly point, for example at an outdoor car park. Personnel presenting their card at the terminal during an emergency are considered safe and accounted for.

If this option is selected, terminals with a display show a message such as 'SWIPE IF SAFE' during the emergency. The exact wording of the message is configured in the **Access Control Parameters** option in CoreAccess. When the emergency is finished, the message displayed by the terminal reverts back to the display text entered above.

[5] Not all turnstile models support this feature.

This button allows you to pin down the window. When this feature is activated you may select other devices in the main program window, while the device property window stays floating on top. This allows you to more quickly review device details.

This button is only present when password(s) have been set (see Setting the User Password on page 22) and hardware / Oracle communication is currently stopped. It shows whether the screen is currently locked or unlocked and allows you to lock or unlock the screen by pressing the button.

If the screen is locked, all fields are greyed out. Press the button and you will be asked for the password.

If the screen was unlocked with the user password, it looks as shown in the screenshot on page 23. To fully unlock the screen, press the button twice and enter the engineer password.

Types of Devices

The screenshot on page 23 shows the most common hardware device screen, used for Benzing access control and T&A terminals. The screens associated with some other types of devices differ, but the fields you may edit as a user are covered above, for all device types.

The possible device types are:

Access Terminal (92xx): A Benzing access control terminal, typically without a display.

T&A Terminal (93xx): A Benzing time & attendance terminal with a display.

Bedanet (9380): A Benzing touch-screen terminal.

BITS (98xx): A Benzing Intelligent Terminal Server. This is a parent device and should have sub-terminal(s) attached to it.

9290 Parent: A Benzing 9290 access control manager parent device. This device should have sub-terminal(s) attached to it.

9290 Child: A Benzing 9290 sub-terminal.

Serial Port: A serial port of the PC, used for Benzing communication.

BETA or BETOR: A Benzing Ethernet or Token Ring adapter. Some Benzing terminals, such as the Bedanet 9340 and 9380 models feature integrated adapters. In this case two devices are listed in the software, a BETA or BETOR device and, indented underneath it, the Benzing terminal device.

ADACS Connection: TCP/IP parameters to link to the ADACS 5 software.

ZMP Parent: An Initial ZMP parent device.

ZMP Child: An Initial ZMP child device.

Terminal details in Oracle

Once you start hardware / Oracle communication again after amending terminal details, these details are automatically saved in the Oracle database.

Note that your version of CoreAccess may still include a legacy screen, the **Access Control / Reference Data / Terminal Identification** option (ACF010), which also allows you to amend terminal details. You should no longer use that screen, but use the Core 2000 Interface instead, since it will overwrite any changes made by the ACF010 screen.

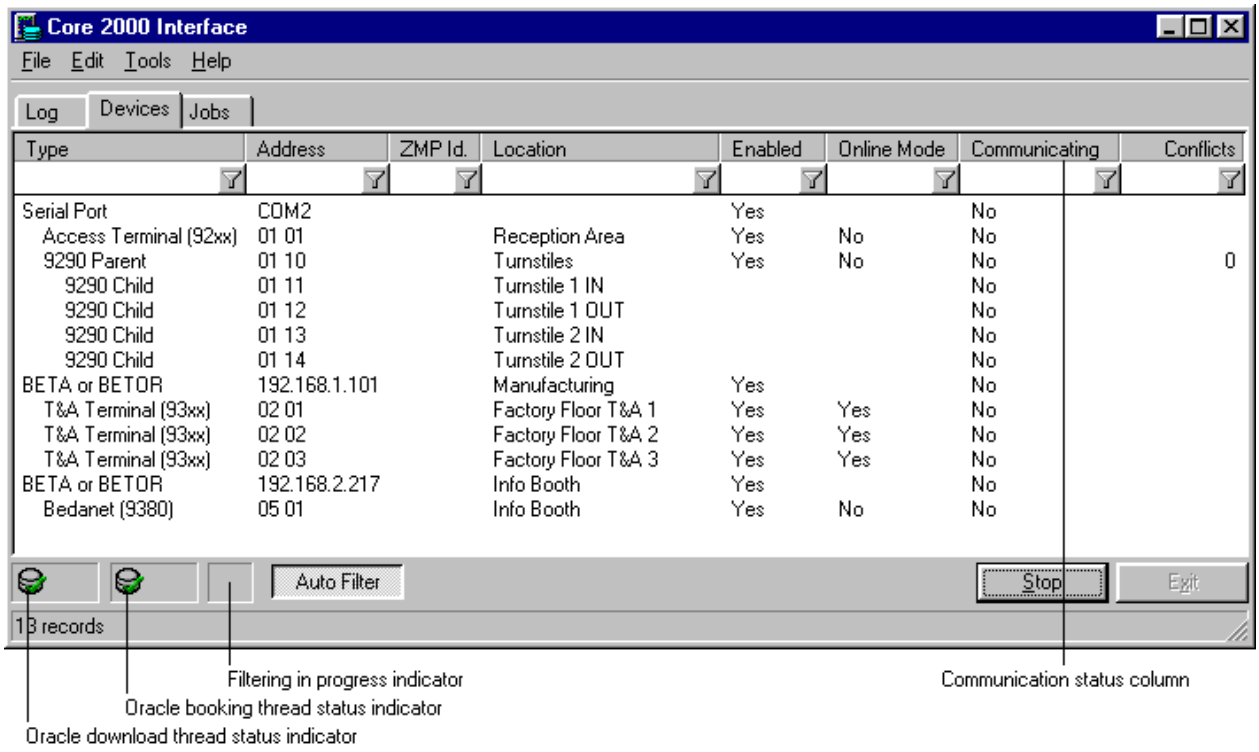
It may also be of interest that the Core 2000 Interface holds more device details than are held in Oracle. The Oracle-based CoreAccess front-end only shows details of card readers, but not details about their parent devices, terminal servers and network adapters, which are handled transparently by the Core 2000 Interface.

Multi-edit

You can select multiple devices of the same or similar type by using the shift and control keys while highlighting a device with the mouse, in the usual manner. Then choose the **Edit Properties** option from the **File** menu. In this case values are only shown, if they are the same for all selected devices. Other values are left blank and tick boxes can show a tick mark on a grey background. You can amend all selected devices simultaneously by filling in non-blank values.

Maintenance

The Main Program Window


Core 2000 Interface
File Edit Tools Help
Log Devices Jobs
Type Address ZMP Id. Location Enabled Online Mode Communicating Conflicts
Serial Port COM2 Yes No
Access Terminal (92xx) 01 01 Reception Area Yes No No
9290 Parent 01 10 Turnstiles Yes No No 0
9290 Child 01 11 Turnstile 1 IN No
9290 Child 01 12 Turnstile 1 OUT No
9290 Child 01 13 Turnstile 2 IN No
9290 Child 01 14 Turnstile 2 OUT No
BETA or BETOR 192.168.1.101 Manufacturing Yes No
T&A Terminal (93xx) 02 01 Factory Floor T&A 1 Yes Yes No
T&A Terminal (93xx) 02 02 Factory Floor T&A 2 Yes Yes No
T&A Terminal (93xx) 02 03 Factory Floor T&A 3 Yes Yes No
BETA or BETOR 192.168.2.217 Info Booth Yes No
Bedanet (9380) 05 01 Info Booth Yes No No
Auto Filter
Stop
Exit
13 records
Filtering in progress indicator
Oracle booking thread status indicator
Oracle download thread status indicator
Communication status column

The above screenshot shows the main program window, the central area of which is taken up by a tabbed dialog with the **Log**, **Devices** and **Jobs** tabs. The **Devices** tab, shown in the screenshot, lists the hardware devices at your site. The columns are:

Type Shows the type of the device. Devices are listed such that connected devices are shown indented underneath their parent devices. For instance, in the screenshot an Access Terminal and 9290 Parent device are both connected to the Serial Port COM2 and hence are indented underneath. The 9290 Parent device in turn has 4 9290 Child devices (readers) connected to it, which are indented further. Please refer to Types of Devices on page 25 for a list of the possible device types.

Address This column varies for different device types. For network adapters it shows the IP-address. For Benzing terminals and ZMPs it shows their GID and DID, which are two numbers identifying the device[6]. For instance the 9290 Parent device in the above screenshot has a GID of 01 and DID 10. The combination of GID and DID is unique throughout the system and unambiguously identifies a device.

ZMP Id. This column only applies to Initial ZMP devices and shows the ZMP Id. and reader number. The reader number is shown in decimal, separated from the ZMP Id. by a colon.

Location Shows the location where the device is installed, see also Location on page 24.

Enabled If applicable, shows whether communication with the device is currently enabled.

Online Mode Shows whether the terminal is configured in online mode. See Online vs. Offline Mode on page 49 for an explanation. This is a static column and does not necessarily mean that the terminal is currently communicating online with the software.

Online mode is 'Pending' after program installation until the software has retrieved badge details and access rights from Oracle.

Communicating Shows whether this device is currently communicating with the software. Please refer to Checking the Hardware Communication Status on page 35 for more information.

Conflicts This column only applies to 9290, BITS and ZMP devices. Please refer to Hardware Compatibility Implementation on page 50.

Further features of the main program window are:

Log tab This tab shows audit information used by service engineers for troubleshooting and, in particular, shows all hardware and Oracle communication. You do not need to examine this tab unless instructed by a service engineer. The program automatically keeps one month worth of audit trails. See also Disk space requirements on page 8.

[6] GID is short for Group IDentification, DID stands for Device IDentification. These terms stem from the historical development of the Benzing terminals and the GID has nothing to do with access groups in Core.

Jobs tab

Jobs are special requests to communicate with the Benzing hardware and require a knowledge of low-level Benzing protocols. This option is reserved for service engineers and is normally only used when hardware is installed or reconfigured. Except when using the Full Reconciliation option (see The Full Reconciliation Option on page 41 in the Database Synchronisation chapter), the software does not create jobs as part of normal operation, though you may find old, completed jobs permanently listed on the Jobs tab. These can be deleted by highlighting the job(s) with the mouse and pressing the Delete key or invoking the Delete option on the Edit menu[7].

Further tabs

If you run the **Show Internal Tables** option on the **Tools** menu, further tabs appear to the right of the **Jobs** tab. These show tables, such as badge details, that the Core 2000 Interface has extracted or in some cases indirectly generated from the Oracle database. The data cannot be modified and is only displayed to aid troubleshooting. You do not need to examine these tabs unless instructed by a service engineer.

The filter bar

The filter bar appears just below the column headings and allows you to select the data that you want to see. For instance, if you only want devices with communication errors to be shown, you should type **No** into the filter field of the Communicating column.

You can specify a comma-separated list of values in a filter field, for instance filtering by **Yes, No** finds all lines containing the word 'Yes' or the word 'No'. The words may appear anywhere within the column and possibly within longer words.

You can specify a range of values with a dash. For instance **AB-AE** finds all lines beginning with the string 'AB' through 'AE'.

To find lines that do not include a value, use the exclamation mark. For instance filtering by **! Yes** excludes all lines containing the word 'Yes'.

You can combine lists and range searches. For instance **AB-AE, Yes, ! Hello** finds all lines beginning with AB through AE or containing the word 'Yes', but excluding the word 'Hello'.

You can filter on multiple columns simultaneously, in which case only the lines where all columns match are shown.

All comparisons are non-case sensitive.

[7] You should only delete completed or failed jobs, not queued or running jobs (as marked in the Status column). It is not necessary to delete old jobs, except for tidiness.

Filter data types Most columns are treated as textual columns, except for date and pure numeric columns.

To filter on date columns, you can enter the dates in the dd/mm/yyyy format, the same format they are displayed in, but you may also use shorthand notations. When using these, the program uses the current system date to fill in the blanks. For instance, if the current date is 08/01/2002, the values **08/01/02**, **08/01**, **08**, or even just **8** are all treated to mean 08/01/2002. Furthermore **7** would be treated to mean 07/01/2002 and **15/2** would be treated as 15/02/2002. Date ranges such as **5-8** may be specified, referring to the 5th to 8th day of the current month.

Numeric columns, such as the badge number, are treated as numeric, so for instance filtering for badge numbers **0-9** shows all badges up to 9. However columns which contain numbers on the majority, but textual or blank values on some other lines, are not treated as numeric. In that case a filter string such as **0-9** finds every line beginning with the text '0-9', i.e. every numeric value, including 10 upwards.

Tip

If the filter bar is not visible, please refer to Common controls update on page 10.

Tip

All tabs (Log, Devices, Jobs…) retain their filters, even if you switch between them. This can be confusing, as well as helpful. Should a tab mysteriously display less information than expected this can be due to an overlooked filter or a filter currently scrolled out of view (sideways). In that case run the **Clear Filters** option on the **Edit** menu to clear the filters on the current tab or run the **Clear All Filters** option to clear the filters on all tabs.

Filtering in progress indicator This panel shows a blinking filter symbol ( ) while filtering is in progress. Filters are applied automatically when you type values into the filter bar.

Auto Filter button All screens refresh automatically when the data changes. Press this button, if you also want filters to be automatically reapplied. This is suitable for the smaller tables, such as the **Devices** tab, where filtering takes little time. In case you are viewing a table with a lot of data, such as the **Profiles** tab, you might turn this option off, because filtering is frequently restarted, without ever reaching completion and showing results[8]. However turning the option off can yield out-of-date results and show rows that no longer match the filter criteria. To reapply

[8] Filtering speed depends on the amount of data in the table, the complexity of the filters and the speed of the machine. It also depends on the particular columns filtered by. Some columns are indexed and allow faster filtering, provided you filter by a single value or single range of values, not a comma-separated list.

filter(s) manually, press one of the filter buttons ( ) in the filter bar. This causes the filters for all columns to be reapplied, regardless which one of the buttons you press.

When you switch to the **Log** tab, the **Auto Filter** button becomes the **Auto Scroll** button. Auto-filtering is never enabled on this tab, instead the button controls whether the screen automatically scrolls to the bottom when new data is appended to the log. Auto-scroll is automatically disabled, if you apply filter(s) on this tab.

The screenshot on page 27 shows the **Auto Filter** button in it's depressed state (auto filtering enabled).

Oracle status indicators

These two panels show whether the program has successfully connected to the Oracle database. Please refer to Checking the Status of the Oracle Connection on page 32 for more information.

Starting and Stopping the Software

You run the program by double-clicking on the shortcut created during installation (see Icon creation on page 10). Once you do this, the main window shown on page 27 appears, but the software does not automatically begin doing any work. It is not yet communicating with the hardware nor logged on to Oracle. In this mode you can configure the software, as described in the Configuration chapter beginning on page 11. Note that, if the software is already running and you double-click on the shortcut, the running copy of the software will be shown. In that case you may have to stop it to enter configuration mode.

Starting the software

To begin hardware and Oracle communication, simply press the **Start** button towards the lower right corner of the program window. You will notice that the button changes and now reads **Stop** and that icons appear in the Oracle status indicator panels. You should check that hardware and Oracle communication is successfully established, as described further below in this chapter.

Stopping the software

To stop the software, simply press the **Stop** button. To exit completely, press the **Exit** button next to it. The software is designed so that it can be stopped or interrupted at any time. Once you restart it, it automatically continues where it left off.

When you stop the software, the hardware devices are switched to offline (stand-alone) mode. Depending on the hardware configuration at your site, this may result in reduced functionality at the terminals, such as an inability to enforce global (site-wide) anti-passback. For a

full description of the differences between online and offline mode, please refer to Online vs. Offline Mode on page 49 . If the software is stopped for an extended period of time (several days), the Benzing terminals may fill up and stop accepting further bookings[9].

It is therefore recommended that the software be kept running at all times, except when it must be stopped to amend the configuration. The software need not and should not be stopped when Oracle is shut down or when the machine is backed up. Please refer to Suspend Oracle Connection on page 12 and to Backing Up on page 43 for further details.

Running the software as a service

If the software is installed as an NT/2000 service, it's behaviour differs from the above described. When you press the **Start** button the program terminates, then restarts itself as a service. A small Core 2000 Interface icon ( ) appears in the status area (sometimes called the system tray) of the taskbar[10].

Click on the icon to start the user interface of the software. You may be asked for a password. To stop the service, bring up the user interface and press **Stop**. The software will terminate. To bring it back into configuration mode you must restart it from the desktop icon.

You can also start and stop the service through the Windows control panel or with the 'net start' and 'net stop' commands. Please refer to Configuring the Software to run as a Service on page 13 for more information.

Checking the Status of the Oracle Connection

Objective

To determine whether the software is successfully logged on to Oracle and to troubleshoot the Oracle connection.

Navigation

Examine the two Oracle status indicators in the bottom left corner of the main program window, shown in the screenshot on page 27. If the software is running as a service, click on the icon in the status area to invoke the user interface first.

Status indicators

There are two status indicators, because the program maintains two connections to the Oracle database.

- The left indicator shows the status and activity of the 'download

[9] The terminals handle this situation in different ways, depending on configuration.
[10] Unless the software is configured as a non-interactive service.

thread', responsible for retrieving access rights and other settings originating in Oracle.

- The right indicator shows the status and activity of the 'booking thread', responsible for saving events in Oracle, such as bookings, originating at the terminals.

The indicators may look as follows:

The Oracle connection is successfully established and is currently idle.

The Oracle connection is successfully established and the software is actively communicating with Oracle. The number to the right indicates what particular query is being executed at the moment. On a fast machine and network you will only occasionally see the indicator going to active status, even though the Oracle connection could be in active use. Only prolonged queries trigger the indicator.

If the indicator permanently shows the same number without any intermediate flickering and you can't stop the software, a record in the database may be permanently locked or there may be an Oracle error. This should not happen.

This symbol is shown in the following cases:

- The Oracle connection is deliberately paused, see Suspend Oracle Connection on page 12.
- You are running a version of Core 2000 Interface executable that does not connect to Oracle. See Program installation on page 9.
- Under Windows 2000 you may also see this symbol in the left indicator panel, but not necessarily the right panel, if the network cable was unplugged while the software was being started[11]. Make sure the network connection is working, then stop and restart the software. If the problem persists, the IP-address of the machine may have been changed, requiring reconfiguration of the Core 2000 Interface. Contact your supplier.

There was an error and the software is not logged on to Oracle. Click on the icon to see a description of the error. Double-click on the icon to attempt to reconnect.

This condition can have many reasons, such as an unexpected Oracle shutdown, Oracle client configuration errors, network errors and so on. It is normal to see this symbol, if the software is running as a

[11] This condition does not occur, if the network cable is unplugged while the software is already running.

service on the database server and the machine was just rebooted, because Oracle might not have been available when the software attempted to log on.

In this condition the software automatically attempts to log back on to Oracle every 15 minutes. Double-click on the icon(s) to attempt to reconnect immediately.

If the panel is blank, this could be due to the following reasons:

- The software is in configuration mode, i.e. you haven't pressed the **Start** button yet. See Starting and Stopping the Software on page 31.
- The Oracle logon is disabled. See Connect to Oracle on page 12.

Checking the Status of the ADACS 5 Connection

Objective To determine whether the software is successfully communicating with ADACS 5 and to troubleshoot the ADACS 5 connection.

Navigation Examine the Communicating column on the **Devices** tab, shown in the screenshot on page 27. If the software is running as a service, click on the icon in the status area to invoke the user interface first.

Notes The communicating column will show 'Yes' or 'No' against the ADACS Connection on the **Devices** tab. You may have to scroll downwards to find the ADACS Connection. If 'No', ping the ADACS machine and make sure ADACS 5 is running. You can also check for the exact error by searching for messages with log type 'Error' and message 'connect ()' on the **Log** tab.

If the connection is lost, the software automatically tries to reconnect to ADACS after a timeout, typically every minute.

Checking the Hardware Communication Status

Objective To determine whether the software is successfully communicating with the hardware devices and to troubleshoot the hardware connections.

Navigation Examine the Communicating column on the **Devices** tab, shown in the screenshot on page 27. If the software is running as a service, click on the icon in the status area to invoke the user interface first.

Notes The Communicating column uses the words 'Yes' and 'No' to indicate whether a device is communicating. You can quickly find any non-communicating devices by typing **N** or **No** into the filter field at the top of the column. If the list turns blank, all devices are communicating properly.

If the column reads 'Yes (full)' the terminal is communicating, but is filled to capacity with master (badge) records. You will find that some badges don't work in offline mode, even though access rights were granted in CoreAccess. Reduce the number of badges having access at the terminal or contact your supplier to configure it for online operation (if not already online) and/or to purchase a memory upgrade.

The Communicating column will be blank (without filtering) for any devices that are deliberately disabled or where their parent device(s) are disabled. This is normal. If all devices show as blank, hardware (and Oracle) communication may not be started. See Starting and Stopping the Software on page 31.

It is normal for devices to show as not communicating at program start until communication has been established. This may take up to one minute, depending on the device and connection types. In case of devices on a serial port, the devices may show as communicating before the serial port itself is marked communicating. This is normal.

If a device is not communicating, please refer to the following list for troubleshooting:

Serial Port Make sure the cable is plugged into the (correct) serial port and that the RS485 converter, if any, is securely plugged into a mains socket and feels warm. Make sure a second cable runs from the converter to an RS485 bus or patch panel.

BETA or BETOR

Try to ping the device, e.g. type 'ping <IP-address>' at a command-prompt. If this succeeds, contact your supplier[12].

If ping fails, check that the network cable is plugged into the machine, then locate the BETA or BETOR network adapter and make sure the power, network and RS485 cables are all plugged in and that lights are showing on the unit. If all cables are plugged in, disconnect the power cable for a few seconds, then reconnect it.

The Bedanet series of terminals feature integrated network adapters. In that case merely make sure the unit(s) are powered up and, in case of a Bedanet 9380, that the Benzing software is running, for instance it is not just showing the Windows desktop.

If ping still fails, there could be a routing problem. Run tracert or other tools for troubleshooting. If this fails to uncover a problem, contact your supplier.

Benzing terminals

First check whether the parent device(s) are also marked as not communicating. In that case the fault lies with the parent device. For instance, if a 9290 Child is marked not communicating and the 9290 Parent device is also not communicating, the fault lies with the 9290 Parent device. If the serial port or BETA / BETOR that the 9290 Parent is connected to is also not communicating, the fault lies with the serial port or BETA / BETAOR.

Otherwise check that the device(s) are powered up. If they are, contact your supplier.

ZMP terminals

Please refer to ADACS 5 for troubleshooting. The status displayed by the Core 2000 Interface merely mirrors the status reported by the ADACS 5 software.

[12] You may be able to ping a device, yet it may not communicate with the Core 2000 Interface, if, for instance, the IP-address of the machine was changed.

Database Synchronisation

Technical Background

This chapter covers ways to force the Core 2000 Interface to synchronise or resynchronise the hardware terminals with the Oracle database. While the software is designed to automatically perform this function, there are special cases where the following options must be run explicitly. These arise during hardware installation, repairs or backup recovery and are usually handled by our service engineers. However the options are also customer accessible. This section provides the technical background to enable you to understand when you might use them.

Databases and database synchronisation

There are 3 layers in the Core architecture at which databases are held:

- At the top application layer is the central Oracle database, holding access control, time & attendance, personnel and payroll information.
- At the middle layer the Core 2000 Interface holds a small subset of the Oracle database, covering badges and access rights.
- At the bottom layer the Benzing and ZMP devices themselves hold a subset of the Core 2000 Interface database, also covering badges and access rights, so the devices can operate in stand-alone (offline) mode, if necessary.

It is the job of the Core 2000 Interface to make sure that these databases are properly synchronised. In particular, if access rights are changed in the Oracle database, the Core 2000 Interface picks up the changes and transmits them to the hardware devices.

Synchronisation steps

There are two discrete steps involved in synchronising the databases:

- The Core 2000 Interface synchronises it's own database to the Oracle database.

- The Core 2000 Interface synchronises the hardware devices to it's own database.

Synchronisation with Oracle

Synchronisation with Oracle happens automatically in the following ways:

- The list of hardware devices, which originates in the Core 2000 Interface, is automatically saved in Oracle whenever the software is started and logs on to Oracle[13].
- The lists of booking types, alarm codes and zones are automatically retrieved and updated whenever the software logs on to Oracle.
- Badges and access rights are automatically retrieved in their entirety when the software is started and logs on to Oracle for the first time after installation. Thereafter the Core 2000 Interface database is updated via triggers in the Oracle database and a special table, called the access queue. When the software is logged on to Oracle, these updates happen automatically within seconds, otherwise update requests are held in the access queue table until the Core 2000 Interface logs on. It then automatically performs the outstanding updates.

Synchronisation of the hardware devices

The Core 2000 Interface automatically synchronises the hardware devices to it's own database. To do this it flags all badges and access rights in it's own database that have recently been added, changed or deleted, and must yet be transmitted to the device(s), as being 'dirty'. The dirty flags are used to keep track of the outstanding updates for each device, rather than having an explicit queue of updates. Once communication with a device is established, the software automatically transmits the outstanding, 'dirty' data.

The Download Terminal Data option in Core

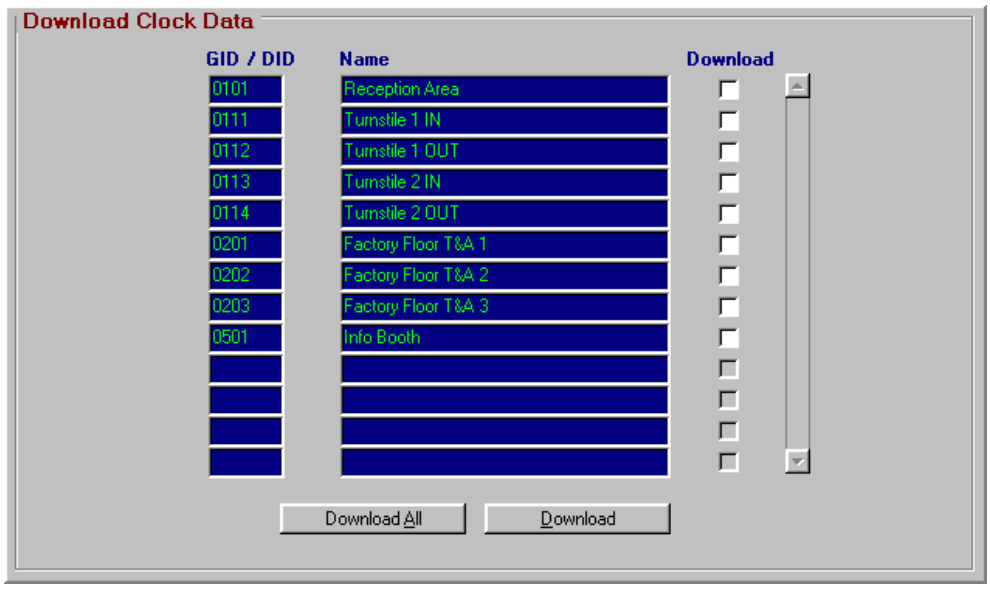
Objective

To force the Core 2000 Interface to download all badges and access rights from Oracle to it's own database (again).

[13] Only details of the access points are stored in Oracle. Details about parent devices and network adapters are not stored, but are exclusively held in the Core 2000 Interface database.

Navigation

Run the **Download Terminal Data** option on the **Access Control** menu in CoreAccess.



You are presented with a list of terminals and two buttons at the bottom of the window, as shown above. Press the **Download All** button and ignore the warning message, if any, about the dangers of running this option[14].

Notes

The option causes full synchronisation with Oracle, including deletion of badges that exist (for whatever reason) in the Core 2000 Interface database, but that no longer exist in Oracle. You can run it at any time, even if the Core 2000 Interface is not running or connected to Oracle. The request is queued and automatically executed (or resumed) when the Core 2000 Interface is started again. One instance, where it may be necessary to run this option, is when a CoreTime site is upgraded to a CoreTime / CoreAccess site.

Performance impact

This option typically has little performance impact and usually takes just a few minutes to complete.

[14] The option could be disruptive with the previous version 1.xx of the Core Interface software, but this is no longer the case with current 2.xx releases, which operate fundamentally differently. The Download Terminal Data screen may also feature a facility to download data to selected terminals only. This is a legacy option, no longer supported by the version 2.xx Core 2000 Interface. Instead use the Database Download option in the Core 2000 Interface, described below.

The Database Download Option

Objective

To force the Core 2000 Interface to download all badges and access rights from it's own database to one or more Benzing terminal(s) (again).

Navigation

In the Core 2000 Interface, select terminal(s) on the **Devices** tab by highlighting them with the mouse and the Shift and Ctrl keys, as usual. You can select multiple terminals of the same or a similar type simultaneously. When you've selected the terminal(s), run the **Database Download** option on the **Tools** menu.

Notes

This option marks all badges and access rights for the selected terminal(s) dirty (again). You can run it at any time, even when the software is not started or the terminal(s) are not currently communicating. Your request is simply queued.

This option adds and updates badges in the terminal(s), but does not necessarily delete badges that exist in a Benzing terminal, yet should no longer have access. It is primarily intended for service engineers in case the system board in a terminal is replaced or the terminal was hard reset and it's memory is known to be empty.

Performance impact

Depending on hardware configuration and the number of personnel who are allowed access, the option can take from several minutes to several hours to complete. During that time terminals may be slower to respond when a badge is presented and, for terminals operating in offline mode, the latest updates of access rights will not come into effect until the downloads triggered by this option have completed.

The Full Reconciliation Option

Objective

To force the Core 2000 Interface to fully synchronise it's own database *and* all enabled terminals to Oracle (again).

Navigation

Run the **Full Reconciliation** option on the **Tools** menu.

Notes

This fully synchronises the Core 2000 Interface database and all enabled[15] terminals to the Oracle database by performing the following steps:

- Download of data from Oracle, as if the above-described Download Terminal Data option was invoked in CoreAccess.
- Download of data to the terminals, as if the above-described Database Download option was invoked in the Core 2000 Interface for each enabled terminal.
- Upload of badges from the Benzing terminals, followed by deletion of badges that should no longer have access. The upload requests are shown on the Jobs tab.

You can invoke the option, whether the software is started or not. If the software is not yet started, the relevant requests are simply queued. If the software is stopped during full reconciliation the process resumes automatically when the software is restarted. You do not need to run the option again.

This option is typically only run after restoring the Core 2000 Interface software from backup.

Performance impact

The option has the combined impacts of the previously described Download Terminal Data and Database Download options. In addition terminals are switched to offline (stand-alone) mode during the badge upload phase.

[15] Terminals can be disabled by our service engineers. Such units are still present on the Devices tab, but the software does not attempt to communicate with them. Terminals are usually only disabled, if they are defective or no longer in use.

Backup and Recovery

Files and Directory Structure

The software consists of a single executable file, as described in Program installation on page 9, and is typically installed in a dedicated directory. When run, it creates the following files and subdirectories:

Corinio.ini Initialisation file storing global settings entered via the Options dialog on the Tools menu. The information in this file mostly remains static.

Database Subdirectory containing local database files. Most of these files are entirely cached in memory and all are kept open while the software is running. They are:

Node.dat:	Contains hardware device details.
Global.dat:	Contains dynamic global data. See also Booking on page 43.
Badge.dat:	Contains badge details.
Person.dat:	Contains personnel details.
Profile.dat:	Contains access rights.
TProfile.dat:	Contains time profiles.
TLevel.dat:	Contains time-level profiles for 9290 and BITS devices.
ZmpTZone.dat:	Contains time zones for ZMP devices.
SpecDay.dat:	Contains special day (holiday) details.
BType.dat:	Contains a list of Benzing booking types.
ACode.dat:	Contains a list of Benzing alarm and error conditions.
Zone.dat:	Contains a list of sites and zones.
Job.dat:	Contains Benzing communication requests, usually only used during setup.

This directory may also contain .FIL files, temporary files used by the filter bar feature of the software.

Booking Subdirectory containing text files with bookings and other events that originated at the hardware devices, stored in native Benzing and semi-native ZMP formats. The software writes events to the intermediate files in this directory, then imports them into Oracle. This usually happens automatically, a few seconds later, unless the Oracle connection is unavailable, in which case the files in this directory store the data until Oracle is available again.

Up to 31 files are stored, labelled with the day of the month that the events occurred at. Files are automatically truncated and re-used after one month, unless they were not yet fully imported into Oracle, in which case the files retain older events until they can be imported. The software keeps track of how much data was already imported into Oracle, and from which files, using the Global.dat file in the Database subdirectory.

Log Subdirectory containing up to one months worth of audit trails in binary files labelled 01.dat through 31.dat, which are displayed by the software on the Log tab. See also Disk space requirements on page 8.

This directory may additionally contain .FIL files, temporary files used by the filter bar feature of the software.

Download Subdirectory containing hardware parameter files used by our service engineers during hardware installation. This directory should be backed up, see Backing Up below.

Backup Subdirectory containing copies of further files that should be backed up. See Backing Up below.

Backing Up

Objective To backup the software so it can be re-installed from the backup and the distribution media in the event of hardware failure.

Background information Due to the nature of the software much of it's data files contain transient or cached information that does not need to be backed up, since it is either temporary or can be reconstituted from the Oracle database. All files in the Log and Booking directories, as well as most files in the Database directory fall into this category.

Files that *do* need to be backed up are the Corinio.ini file in the main directory and the Node.dat file in the Database subdirectory, which contain important configuration information. These files are

automatically copied into the Backup subdirectory whenever a configuration change could have been made. You should backup the copies in the Backup subdirectory rather than the original files, since the original files may frequently be open and impossible to back up.

The program does not store important information in the registry[16], nor any information elsewhere on the hard disk, but in it's own directory, where the executable is located, and subdirectories. This makes it possible to easily restore or move it to a different location, without amending any configuration files.

Core 2000 Interface backup

You should backup all files in the Download and Backup subdirectories. These files need only be backed up after a configuration change, such as the installation of additional hardware. However it may be more convenient to simply include them in the regular (daily) backups of the machine.

You should not backup files from the other subdirectories, nor the parent directory where the executable is installed. The Core 2000 Interface should not be stopped during a backup (see also Stopping the software on page 31). Because the software will be running, attempting to backup the other files might fail and/or interfere with the correct operation of the software.

Oracle backups

You should not stop the Core 2000 Interface during Oracle database backups. If the Oracle database is taken down for backups, use the scheduler option, described under Suspend Oracle Connection on page 12, to make the software disconnect gracefully from Oracle during those times.

Restoring a Backup

To reinstall the software from a backup follow these steps:

1. **Machine selection** — You may restore the software onto any suitable machine, as per the Requirements listed from page 6 onwards.

2. **IP-address(es)** — The machine must have the same IP-address(es) as the original one[17].

[16] A few, unimportant user preferences, such as user interface window sizes and positions, are stored in the registry.
[17] If different IP-address(es) should be used, this requires reconfiguration of the software as well as the Benzing hardware devices. Contact your supplier.

3. **Serial port(s)** — If Benzing terminal(s) are connected via the serial port, make sure the serial cable is plugged into the machine. It should be plugged into the same port as before (COM1, COM2…).

4. **Oracle restoration** — Restore your Oracle database from backup, if necessary, and start the database.

5. **Installation** — Follow the instructions in the Installation section on page 9 to install the software from the distribution media. You do not need to choose the same drive or directory as the original installation, though doing so may simplify the next step. Do not yet run the software.

6. **Backup restoration** — Restore the **Download** and **Backup** subdirectories from your backup media, then copy the Corinio.ini file from the **Backup** subdirectory into the main directory, where the Corinio*n*.exe executable is installed. Create a subdirectory named 'Database' and copy the Node.dat file from the **Backup** subdirectory into the **Database** subdirectory.

7. **Time check** — Make sure the machine's date and time are correctly set. This can usually be done by double-clicking on the time in the bottom right corner of the screen.

8. **Restoration check** — Run the Core 2000 Interface software and inspect the **Devices** tab, making sure that it is not blank and your hardware device details have been restored. Next invoke the **Options** dialog from the **Tools** menu and make sure these settings have also been restored. For instance the Oracle user and password should not be blank.

9. **Oracle host** — If the Oracle client installation on the new machine differs from the original one, you may need to amend the Oracle host string in the **Tools / Options / Oracle** dialog.

10. **NT/2000 service** — If the program should run as an NT/2000 service, you must re-enable this option. See Configuring the Software to run as a Service on page 13.

11. **Review settings** — Review the **Import File** setting on the **Primary Settings** tab in the **Tools / Options** dialog and the **Destination** and **Core Forms Directory** on the **Roll Call** tab. Make sure these settings comply with the network drive and printer mappings of the (new) machine. Please refer to Importing T&A Bookings During a Parallel Run on page 16 and Configuring an Automatic Roll Call Report on page 20 for details about these options.

12. Full reconciliation Run the **Full Reconciliation** option on the **Tools** menu. This option ensures that the Core 2000 Interface database becomes fully synchronised with the Oracle database and with all the Benzing devices again, once the software is started. For technical background information, please refer to the Database Synchronisation chapter on page 37.

13. Disable ADACS If you have ZMP devices, you must (temporarily) disable the ADACS Connection on the **Devices** tab by double-clicking on this entry and removing the tick-mark from the **Enabled** field.

14. Start the software Press the **Start** button. Refer to the Maintenance chapter on page 27 for more details on starting the software and checking the status.

15. Re-enable ADACS If you have ZMP devices, you should re-enable the ADACS Connection once the Core 2000 Interface has retrieved all badge details from Oracle. You can determine this by switching on the **Show Internal Tables** on the **Tools** menu, then switching to the **Badges** tab and running the **Clear Filters** option on the **Edit** menu. The software is finished once the number of records, displayed at the bottom of the screen, stops increasing. You must stop the software to re-enable ADACS, then start it again.

16. ZMP downloads If you have ZMP devices, you should run the Request Card Download option in ADACS 5, for all ZMPs, once the Core 2000 Interface has retrieved all badge details from Oracle.

17. Test roll call If you are using the Core 2000 Interface to automatically run fire alarm-activated roll reports, you should run a test report. To do this activate the fire alarm, if possible[18]. Alternatively stop the software and invoke the **Tools / Options / Roll Call** dialog. Press the **Test** button.

Important You should not restore files other than those mentioned above, even if other files could be recovered from the original installation. In particular you should not restore the Booking subdirectory, since this could cause duplicate time & attendance bookings to be imported into Oracle. If the Oracle database was also restored from backup and bookings are missing in Oracle, please refer to Re-importing Bookings into Oracle on page 47.

[18] The fire alarm may not trigger the report immediately while the full reconciliation is in progress. If possible the test should be performed on the following day.

Re-importing Bookings into Oracle

Objective To re-import missing bookings and other events into the Oracle database.

Rationale The Core 2000 Interface keeps a backup of one months worth of event details, chiefly bookings, from the hardware devices in the Booking subdirectory. In case the Oracle database was lost or corrupted, these bookings can be re-imported into Oracle. It is not required to run this option during normal operation, since events are automatically imported into the Oracle database.

Navigation Run the **Import Bookings...** option on the **File** menu. You will be presented with a standard Windows dialog allowing you to pick files from the Booking subdirectory. Each file is labelled with a day of the month as the filename, 01.txt through 31.txt, and contains bookings and other events from that day. You should press the Details button in the top right corner of the dialog, which allows you to inspect the dates when the file(s) were last written to, and thus the month that they were written. Pick the file(s) you want to import, then press **Open**, but read the remainder of this section first!

Handling of duplicates The option automatically imports bookings and other events into the CoreAccess event table, the CoreTime event table or both tables, depending on the event type. Duplicate events are not imported. It is thus safe to import files even if, say, only half a days data is missing in Oracle or data is missing in only one subsystem (CoreAccess or CoreTime).

Import summary

A summary screen, displayed at the end, lists the number of events imported. Events are classified as follows:

Imported: Events that were imported.

Duplicate: Duplicate events that already existed in the Oracle database (not imported).

Rejected: T&A booking attempts that were rejected by the Benzing terminal or Core 2000 Interface, for instance because the employee was not allowed to book at the particular terminal. Such bookings are not imported into CoreTime.

Ignored: Event types that are deliberately configured to be ignored (not imported) in the Benzing Transaction Types option in Core.

Not set up: Event types that are not set up in the Benzing Transaction Types option in Core. These are not imported.

Other: Invalid or blank lines in the source file. The file you are trying to import may not be a booking file.

Importing from other locations

You are not restricted to importing files only from the Booking subdirectory. For instance you can import files created by older software (B-Comm / CoreTime Interface, B-Comm) elsewhere on the disk.

In case you have restored the Core 2000 Interface from backup and recovered booking files from the previous installation, you should not copy the old files into the Booking subdirectory, but restore them into a different directory, elsewhere on the hard disk or, where possible, import them straight from the backup media (floppy, CD). See also Restoring a Backup on page 44 and Booking on page 43.

Considerations for importing into CoreTime

Special care must be taken when (re-)importing booking files into CoreTime. You should not usually import files where later bookings already exist in CoreTime, and the files must be imported in the correct order by date. To do this it is recommended that you do not pick multiple import files in the file selection dialog, but import the files one by one, running the Import Bookings… option repeatedly, separately for each file. Please contact the Core help desk for further assistance.

Additional Information

Online vs. Offline Mode

The Benzing terminals and ZMP devices are both capable of operating in stand-alone mode, also called offline mode, or in online mode. In the latter case the Core 2000 Interface validates access attempts and responds to the devices in real-time; the terminal transmits the booking to the Core 2000 Interface, then waits for a response from the Core 2000 Interface, which indicates whether the booking should be accepted or not.

Online mode makes it possible to implement features, such as global anti-passback, which the terminals cannot perform in isolation. The following table provides a comparison of features available in online mode, implemented in software at the Core 2000 Interface level, and in offline mode, implemented at the hardware level. It is worth noting that the terminals automatically switch to offline mode, if the communication with the software breaks down.

Feature	Online	Offline
Access control by badge	Yes	Yes
Access control by time of day / day of week	Yes	Yes
Bank holidays / special days	Yes	Benzing models only
PIN numbers	Yes	Yes
Display name when badge is booked	Yes	Some high-end models (9380, BITS)
Display visitor company	Yes	No
Display IN/OUT	Yes	No
Display flexitime balances	Yes	Some Benzing models[19]

[19] Not if the communication with the Core 2000 Interface breaks down for a prolonged time.

Feature	Online	Offline
Display notification messages	Yes	No
Enforce expiry dates	Yes	Yes, via downloads[19]
Enforce anti-passback	Site-wide	Limited[20]
Enforce double-access block	Site-wide	Locally[21]
Door control	Yes	Yes[22]
Response time	Fast	Very fast
Update time when access rights change	Very fast	Fast
Max. badge capacity	100,000	Depends on model and memory fitted (0 - 30,000)

Hardware Compatibility Implementation

The basic functionality of the CoreAccess subsystem is modelled on the capabilities of standard Benzing terminals, such as the 9340 model. Features such as the time profile implementation are derived directly from Benzing standards. However Benzing supply a wide range of terminals with different capabilities and the Initial Shorrock ZMP devices, while utilising similar concepts, incorporate a further, different implementation.

The Core 2000 Interface hides these differences and allows CoreAccess to provide a consistent access control model, regardless of the attached hardware. This model is most fully enforced when the hardware is operated in online more. It allows complex combinations of access rights to be set up that in some cases cannot be handled by the hardware in offline (stand-alone) mode, because the devices structure the access control data differently internally and they have different limits with regard to the complexity of supported access rights. While these limits are rarely encountered in practice, a description is nonetheless necessary. The following models are affected:

Benzing 9290

- CoreAccess allows you to configure up to 7 time pairs in a time profile and to assign a different time profile to each 9290 reader. Since there may be up to 8 readers, CoreAccess supports a

[20] Anti-passback can be enforced in a local area with a BITS. It can also be enforced by individual Benzing terminals, though this is rarely practical.
[21] Based on a timer, this can be enforced by individual Benzing terminals.
[22] This is implemented via (scheduled) downloads and requires the Core 2000 Interface to communicate with the hardware. Only the 9290 model also supports scheduled door opening while communication with the software has broken down. Not available with ZMPs through Core Access, but may be available through ADACS 5.

theoretical maximum of 56 distinct time pairs between them, for the same badge. However the 9290 only supports 7 distinct time pairs across all 8 readers, for the same badge. If more than 7 distinct time pairs are used, the 9290, when operating in offline mode, will not permit access at all the times during the day configured in CoreAccess.

- CoreAccess theoretically allows you to configure different access rights for each and every badge in the system. The 9290 however only allows up to 99 distinct combinations of readers and time zones to grant access by. If more than 99 distinct combinations are used, some badges may not permit access in offline mode.

Benzing BITS

- If there are more than 16 sub-terminals connected to a BITS, the terminals must be grouped into 16 (or fewer) groups[23] and all terminals in a group must be given the same access rights for the same badge. If this is not done, the access rights given to one random terminal from the group will be used for all terminals in the group.

- CoreAccess allows you to configure up to 7 time pairs in a time profile and to assign a different time profile to each of the BITS sub-terminals. Since there may be up to 60 sub-terminals, CoreAccess supports a theoretical maximum of 420 distinct time pairs between them, for the same badge. However the BITS only supports 7 distinct time pairs across all sub-terminals, for the same badge. If more than 7 distinct time pairs are used, the BITS will not, in stand-alone mode, permit access at all the times during the day configured in CoreAccess.

- CoreAccess theoretically allows you to configure different access rights for each and every badge in the system. The BITS however only allows up to 254 distinct combinations of sub-terminals and time zones to grant access by. If more than 254 combinations are used, some badges may not permit access in offline mode.

ZMP models

- ZMPs have up to 16 attached card readers and only allow a single time profile for all the readers, for each badge. If different time profiles are set up in CoreAccess for readers on the same ZMP, one of the time profiles will be picked at random and used for all the readers in offline mode.

- ZMPs do not support time profiles with more than 4 time pairs in a single day. If more then 4 time pairs are used, the ZMP will not, in offline mode, permit access at all the times during the day

[23] These are BITS groups, sometimes called BITS levels, and are not related to access groups in CoreAccess nor to GIDs.

configured in CoreAccess.

- ZMPs support a maximum of 16 time profiles. CoreAccess allows you to set up more time profiles than this and the Core 2000 Interface handles this by only sending a ZMP the time profiles it actually needs. As long as no more than 16 time profiles are used per ZMP, this is not a problem, but otherwise cards that use the 17'th and further time profile cannot be downloaded to the ZMP and are denied access in offline mode.

- ZMPs do not support different access rights on special days (bank holidays etc.) in offline mode.

It should be noted again that most of these limits are of a theoretical nature and rare in practice. In case they do arise, the Core 2000 Interface counts the number of occurrences, for each terminal, where it could not fully translate the access rights into the terminal's own format for offline operation. These counters are displayed in the Conflicts column shown in the screenshot on page 27. Should any of the counters be non-zero, follow these steps to find the affected badges:

1. Switch on the **Show Internal Tables** option on the **Tools** menu.
2. Select the **Profiles** tab.
3. Disable the auto filter option. The **Auto Filter** button at the bottom of the screen should not be depressed.
4. Run the **Clear Filters** option on the **Edit** menu.
5. Type **Yes** into the filter field at the top of the **Level Conflict** column.
6. Wait for the results (list becomes blank or shows rows with Level Conflict 'Yes').
7. Note the affected badge numbers and GIDs and DIDs and examine the badges in CoreAccess, reviewing both their access overrides and access group to determine whether the complex access rights granted to the badge are necessary.
8. Repeat steps 4 through 7 for the **Time Pair Conflict** and **Profile No. Conflict** columns.

The columns are as follows:

Level Conflict	Two or more terminals on the same BITS level were given different access rights or two or more readers attached to the same ZMP were given different time profiles.
Time Pair Conflict	There are too many time pairs in the (combined) time profile(s) assigned to this badge. This condition can arise with 9290, BITS and ZMP devices, as described above.
Profile No. Conflict	There are too many distinct combinations of access rights between the total badges assigned to this 9290 or BITS device, as described above.